(19) Japan Patent Office (JP) (12) Japanese Laid-open Patent Publication (A) (11) Publication No. 2002-324219

(43) Publication date: November 8, 2002

(51) Int.Cl.	ID No.	FI	Theme code (as a reference)
G 06 K 17/00		G 06 K 17/00	S 2C005
B 42 D 15/10	501	B 42 D 15/10	501L 5B058
G 06 F 15/00	330	G 06 F 15/00	330G 5B085

Request for examination: Not requested The number of claims: 7 OL (Total 6 pages)

(21) Application No.: 2001-126416

(22) Filing Date: April 24, 2001

(71) Applicant: 000002325
Seiko Instruments Inc.
8, Nakase 1-chome, Mihama-ku,
Chiba-shi, Chiba, Japan

(72) Inventor: Hitoshi TACHIBANA
c/o Seiko Instruments Inc.
8, Nakase 1-chome, Mihama-ku,
Chiba-shi, Chiba, Japan

(74) Agent: 100096378
Masaaki SAKAGAMI

F-term (as a reference): 2C005 HA03 HB09 HB2
JB33 LB32 LB36
5B058 CA27 KA27 KA02 KA04 KA33 YA02
5B085 AE12 AE23 BA06

(54) Title: CARD AUTHENFICATION SYSTEM

(57) Abstract:

PROBLEM: To provide a card authentication system that is able to prevent illegal use by forgery to a high degree.

SOLUTION MEANS: A card authentication system that is provided with a plurality of card authenticating terminals 10 and a central data processing center 20 connected to these card authenticating terminals via a public communications network 30 and is able to perform online authentication processing at the card authenticating terminals 10 by accessing host computers of the respective card companies 51-53 online from the central data processing center 20 via a card business comprehensive network system 50; wherein it has a usage permitted/not permitted information storage apparatus 40 by which the users of the respective cards are able to switch the validity/invalidity of said cards in advance, and the central data processing center 20 performs online authentication only for cards for which a usage permitted judgment has been made via the usage permitted/not permitted information storage apparatus 40.

CARD AUTHENTICATION SYSTEM

CLAIMS

What is claimed is:

1. A card authentication system that is provided with a number of card authenticating terminals and a central data processing center connected to these card authenticating terminals via a public communications network and that is made to perform online authentication processing at the card authenticating terminals by accessing host computers of the respective card companies online from the central data processing center via a card business comprehensive network system, comprising

a usage permitted/not permitted information storage apparatus by which the users of the respective cards are able to switch the validity/invalidity of said cards in advance, wherein the central data processing center performs online authentication only for cards for which a usage permitted judgment has been made via the usage permitted/not permitted information storage apparatus.

2. A card authentication system of claim 1, wherein the usage permitted/not permitted information storage apparatus receives a card user's request for a change to usage permitted and validates usage for said card.

3. A card authentication system of claim 2, wherein after the usage permitted/not permitted information storage apparatus has received a card user's request for a change to usage permitted and has validated usage for said card, a change to usage not permitted is automatically made at a predetermined time.

4. A card authentication system of any of claims 1 to 3, wherein characterized in that the usage permitted/not permitted information storage apparatus receives a card user's request to change to usage permitted via a user's wireless communications terminal.

5. A card authentication system of any of claims 1 to 3, wherein characterized in that the usage permitted/not permitted information storage apparatus receives a card user's request for a change to usage permitted from a user's wireless communications terminal via the card authenticating terminal.

6. A card authentication system of any of claims 1 to 5, wherein characterized in that the usage permitted/not permitted information storage apparatus has data regarding the respective cards in advance and registers usage permitted/not permitted for the registered cards.

7. A card authentication system of any of claims 1 to 5, wherein the usage permitted/not permitted information storage apparatus registers at any time only data for those of the respective cards that are usage permitted.

DETAILED DESCRITION OF THE INVENTION

TECHNICAL FIELD OF THE INVENTION

[0001] The present invention relates to a card authentication system that makes it possible for the actual user of a credit card or a debit card to set usage permitted/not permitted for said card to prevent illegal usage with, for example, usage only being permitted when used by the rightful cardholder.

PRIOR ART

[0002] Conventional credit cards and debit cards are in principle always usage permitted when a card is issued, except for cards for which usage has been made invalid, such as stolen cards, and cards that have exceeded the usage limit amount and are such that, at the time of usage, usage is permitted after the rightful cardholder's identity has been confirmed.

PROBLEMS TO BE SOLVED BY THE INVENTION

[0003] However, there is no problem if reporting has been performed immediately after theft or loss, but there are cases in which time passes before a report is made, and illegal use cannot be prevented. In addition, conventionally, there has been no protection at all against illegal usage by means of counterfeit cards.

[0004] The present invention takes such circumstances into account, and its purpose is to provide a card authentication system that is able to prevent illegal usage by forgery to a high degree.

MEANS TO SOLVE PROBLEMS

[0005] The first mode of the present invention to resolve the problems is a card authentication system that is provided with a plurality of card authenticating terminals and a central data processing center connected to these card authenticating terminals via a public communications network and is able to perform online authentication processing at the card authenticating terminals by accessing host computers of the respective card companies online from the central data processing center via a card business comprehensive network system; wherein it has a usage permitted/not permitted information storage apparatus by which the users of the respective cards are able to switch the validity/invalidity of said cards in advance, and the central data processing

center performs online authentication only for cards for which a usage permitted judgment has been made via said usage permitted/not permitted information storage apparatus.

[0006] The second mode of the present invention is a card authentication system according to the first mode; characterized in that the usage permitted/not permitted information storage apparatus receives a card user's request for a change to usage permitted and validates usage for said card.

[0007] The third mode of the present invention is a card authentication system according to the second mode; characterized in that, after the usage permitted/not permitted information storage apparatus has received a card user's request for a change to usage permitted and has validated usage for said card, a change to usage not permitted is automatically made at a predetermined time.

[0008] The fourth mode of the present invention is a card authentication system according to any of the first through third modes; characterized in that the usage permitted/not permitted information storage apparatus receives a card user's request to change to usage permitted via a user's wireless communications terminal.

[0009] The fifth mode of the present invention is a card authentication system according to any of the first through third modes; characterized in that the usage permitted/not permitted information storage apparatus receives a card user's request for a change to usage permitted from a user's wireless communications terminal via the card authenticating terminal.

[0010] The sixth mode of the present invention is a card authentication system according to any of the first through fifth modes; characterized in that the usage permitted/not permitted information storage apparatus has data regarding the respective cards in advance and registers usage permitted/not permitted for the registered cards.

[0011] The seventh mode of the present invention is a card authentication system according to any of the first through fifth modes; characterized in that the usage permitted/not permitted information storage apparatus registers, at any time, only data for those of the respective cards that are usage permitted.

[0012] According to the relevant present invention, it is possible to provide a card authentication system that is able to prevent illegal usage due to forgery to a high degree.

EMBODIMENTS OF THE INVENTION

[0013] The present invention will be described below based on an embodiment.

[0014] An overall schematic configuration of an embodiment of a credit card authentication system relating to the present invention is shown in Fig. 1. As shown in Fig. 1, a plurality of card authenticating terminals 10 are connected via a central data processing center 20 and a wired or wireless public communications network 30, and the central data processing center 20 is connected to a usage permitted/not permitted information storage apparatus 40 and a card business comprehensive network system 50 via a leased line communications network. The card business comprehensive network 50 is typically CAFIS of the Card [sic] NTT Data Corporation, and it connects a plurality of card companies 51-53 and financial institutions online.

[0015] The card authenticating terminal 10 has as its principal components a CPU 11, which performs various computations and control, a ROM 12, in which programs are stored, a RAM 13, which stores various data, a card reader 14, which is able to read the member information and the card ID of a credit card requiring authentication, an input/output means 15, which inputs information such as charges and payment methods, a display 16, which displays, for example, the authentication results, a printer 17, by which, for example, usage fees are printed out, and a transmitting and receiving apparatus 18, which is for connecting with the public communications network 30.

[0016] The central data processing center 20 has as its principal components a central processing apparatus 21, which performs various computations and control, a program storage apparatus 22, in which programs have been stored, a data storage apparatus 23, which stores various data, and a transmitting and receiving apparatus 24, which is for connecting with the public communications network 30 while connecting with the card business comprehensive network system 50.

[0017] The usage permitted/not permitted information storage apparatus 40, as shown in Fig. 2(a), comprises a central processing apparatus 41, which performs various computations and control, a program storage apparatus 42, in which programs are stored, a data storage apparatus 43, which stores various data, a transmitting and receiving apparatus 44, which is for connecting with the central data processing center 20, and an acceptance apparatus 45, which receives information directly from a communications terminal 60 such as a portable telephone or a PHS,

and a usage permitted/not permitted information database 46 is stored in the data storage apparatus 43.

[0018] The usage permitted/not permitted information database 46, as shown in Fig. 2(b), is a database in which card numbers and information for access by a user, for example, the member name and password, are registered when, for example, issuing cards such as credit cards, and also comprises information such as whether or not the respective cards are valid or invalid.

[0019] Here, the validity/invalidity information of the usage permitted/not permitted information database 46 can be changed at any time by the user. The method of changing by the user is not particularly limited, but changes may be made via the web connected via a communications terminal, changes may also be made by receiving mail from the communications terminal 60, or changes may also be made by a voice instruction from a communications terminal.

[0020] In addition, changes to the validity/invalidity are such that if there is a validation request, it is made valid, and if there is an invalidation request, it is made invalid, and it is preferable that, after there has been a validation request, there be automatic invalidation after validation for prescribed period of time, for example, a short period of time such as 2 [min.], 3 min., 5 min. or 10 min., or for a prescribed period of time such as one day. This is to prevent illegal usage of counterfeit cards by validating only for the time that the user is engaged in usage.

[0021] Note that it is preferable that the acceptance apparatus 45 accept only validation requests from legitimate users and request prescribed passwords for access so that illegal requests from illegal users are not accepted, and originating party notification of the communications terminal may also be assigned a password.

[0022] In order for a validation request to be performed easily by a user while preventing such illegal usage, for example, a card number, a password that has been registered in advance, and prescribed member information may be transmitted along with a validation request using a mail function of a communications terminal. In addition, an application such as would be able to perform prescribed encryption processing (one-way computation) may be stored in the communications terminal, the result of having performed prescribed encryption processing using the member number of the card and an encryption key registered in advance may be used as a

password, and this may be transmitted along with prescribed member information and the validation request using mail functions.

[0023] In addition, the numbers of only valid cards may also be caused to be present in the usage permitted/not permitted information database 46. Specifically, in the case in which the acceptance apparatus 45 registers only card numbers accepted along with a validation request in the usage permitted/not permitted information database 46, and the card number is present in the usage permitted/not permitted information database 46, the card is considered to be valid. Note that, in this case, in order to prevent access by illegal users, it is necessary to eliminate illegal registration by, for example, issuing a password such that there will be a prescribed result when prescribed encryption processing has been performed at the time of card issuance, for example, a password such that zero always results when a prescribed calculation is performed, and making it so that only card numbers that have been transmitted along with such a password are registered.

[0024] In the card authentication system described above, in the case in which a card is to be used, it is necessary for the user to transmit a validation request to the acceptance apparatus 45 of the usage permitted/not permitted information storage apparatus 40 via a communications terminal such as a portable telephone in advance and preferably immediately prior to usage. After that, that user receives a check as to whether or not usage is possible by means of a card authenticating terminal 10 that is installed at a store or service counter. Specifically, as shown in Fig. 3, the card authenticating terminal 10 reads member information and a card number using the card reader 14 (step S11). This is transmitted to the central data processing center 20 from the transmitting and receiving apparatus 18 via the public communications network 30 (step S12). When the central data processing center 20 receives the card information requiring authentication, it makes a request to the usage permitted/not permitted information storage apparatus 40 as to whether or not usage of said card is permitted and waits for reception of the usage permitted/not permitted decision result (step S13). A judgment is made as to whether or not usage of said card is permitted according to the usage permitted/not permitted decision result (step S14), and in the case in which usage is not permitted (step S14, No), a decision of usage not permitted is made with usage not permitted going to the card authenticating terminal (step S15).

[0025] On the other hand, in the case in which usage is permitted (step S14, Yes), the received member information of the card requiring authentication and the member information from the

card number are separated, and this is converted into prescribed formatted data and transmitted to a prescribed card company via the card business comprehensive network system 50 (step S16), and there is a wait for an authentication result from the card company (step S17).

[0026] When an authentication result from the card company is received, a judgment is made as to whether or not the card requiring authentication is an invalid card (step S18), and in the case in which it has been judged to be an invalid card (step S18, Yes), a usage not permitted determination is made (step S15), and when it has been judged not to be an invalid card (step S18, No), it is judged to be valid (step S19), and information to the effect that authentication is to be performed is transmitted to the card authenticating terminal 10 (step S20). Note that processing of data such as the usage amount and payment method is the same as in ordinary processing of credit cards and debit cards, so a description will be omitted.

[0027] According to the embodiment described above, it is possible to validate card usage only during the period when the user is using the card, so it is possible to prevent illegal usage of the card resulting from, for example, a counterfeit card.

[0028] Note that, in the embodiment described above, in the case in which the user has made a request to change card usage permitted/not permitted, there was direct transmission from the communications terminal 60 to the usage permitted/not permitted information storage apparatus 40, but transmission to the card authentication terminal 10 may also be performed, and transmission from the card authentication terminal 10 to the usage permitted/not permitted information storage apparatus 40 via the central data processing center 20 may also be performed. In this case, the communications terminal 60 and the card communications [sic] terminal 10 may be made able to communicate by, for example, automatically connecting using a wireless standard such as Bluetooth.

[0029] In addition, in the embodiment discussed above, the usage permitted/not permitted information storage apparatus 40 was installed separately from the central data processing center 20, but it goes without saying that it may also be installed within the central data processing center 20.

EFFECTS OF THE INVENTION

[0030] As described above, according to the present invention, an effect is exhibited whereby it is possible to provide a card authentication system that is able to prevent illegal usage resulting from forgery to a high degree.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1

Figure 1 is a drawing that shows the schematic configuration of a card authentication system relating to an embodiment of the present invention.

Fig. 2

Figure 2 is a drawing that shows an overview of the usage permitted/not permitted information storage apparatus of the present invention.

Fig. 3

Figure 3 is a drawing that shows the procedure for authentication of a card authentication system relating to an embodiment of the present invention.

DESCRIPTIONS OF SYMBOLES

10: Card Authenticating Terminal

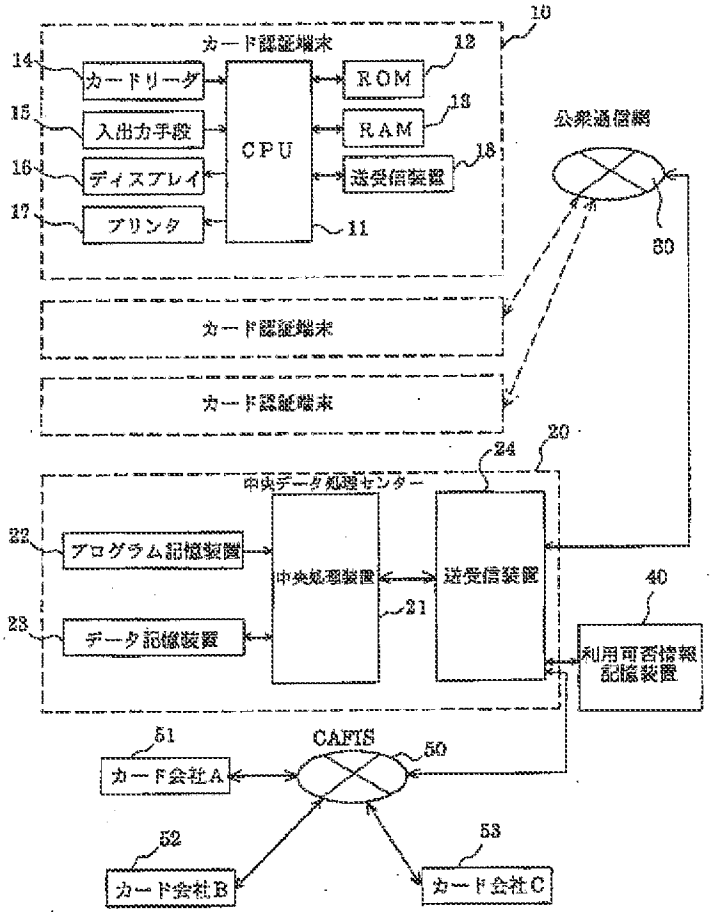
20: Central Data Processing Center

30: Public Communications Network

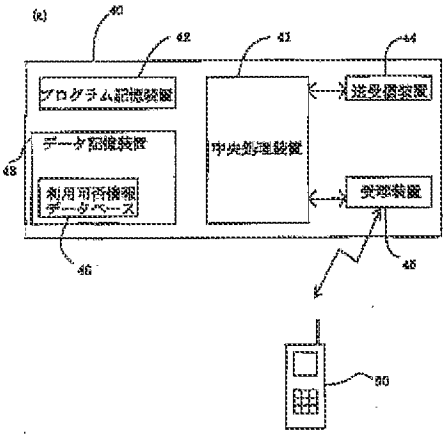
40: Usage Permitted/Not Permitted Information Storage Apparatus

50: CAFIS

【図１】



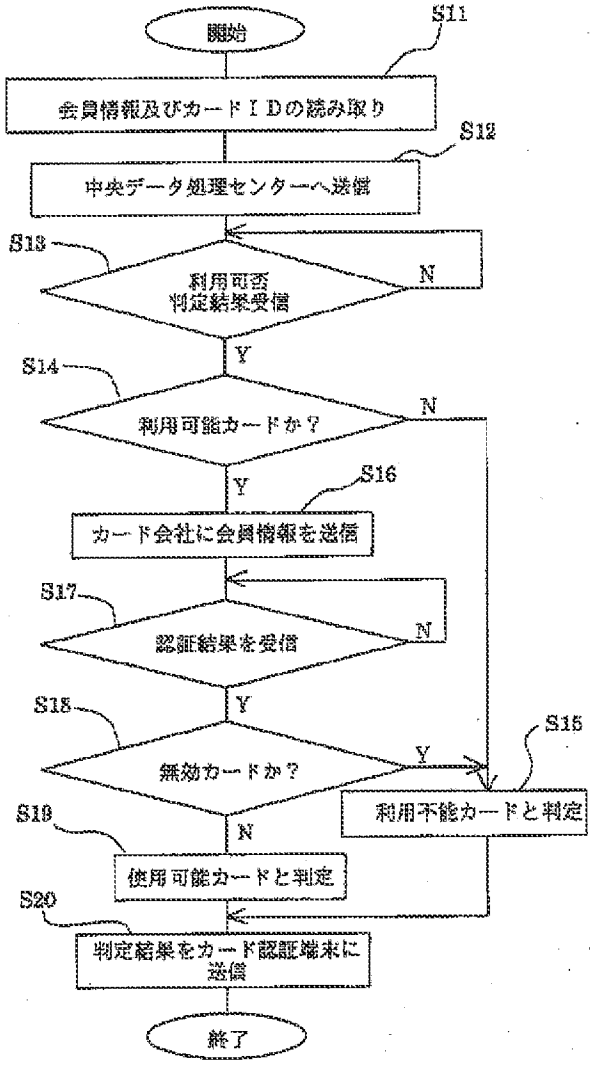
【図２】



(b)

No	カード番号	有効	紛失
1	1234567890	✓	
2	0876543210		✓
3	1111222333		✓
4	4444555666	✓	
⋮			

【図３】


開始
S11
会員情報及びカードＩＤの読み取り
S12
中央データ処理センターへ送信
S13
利用可否
判定結果受信
N
Y
S14
利用可能カードか？
N
Y
S16
カード会社に会員情報を送信
S17
認証結果を受信
N
Y
S18
無効カードか？
Y
S15
利用不能カードと判定
N
S19
使用可能カードと判定
S20
判定結果をカード認証端末に
送信
終了

AMENDMENT

Filing Date: November 19, 2007

Modification of The Entire The Claims

CLAIMS

What is claimed is:

1. A card authentication system that is provided with a plurality of card authenticating terminals and a central data processing center connected to said card authenticating terminals via a public communications network and that performs online authentication processing at the card authenticating terminals by accessing host computers of the respective card companies online from the central data processing center via a card business comprehensive network system, comprising

a usage permitted/not permitted information storage apparatus by which the users of the respective cards are able to switch the validity/invalidity of said cards in advance, wherein the central data processing center performs online authentication only for cards for which a usage permitted judgment has been made via the usage permitted/not permitted information storage apparatus.

2. A card authentication system of claim 1, wherein the usage permitted/not permitted information storage apparatus receives a card user's request for a change to usage permitted and validates usage for said card.

3. A card authentication system of claim 2, wherein after the usage permitted/not permitted information storage apparatus has received a card user's request for a change to usage permitted and has validated usage for said card, a change to usage not permitted is automatically made at a predetermined time.

4. A card authentication system of any of claims 1 to 3, wherein characterized in that the usage permitted/not permitted information storage apparatus receives a card user's request to change to usage permitted via a user's wireless communications terminal.

5. A card authentication system of any of claims 1 to 3, wherein characterized in that the usage permitted/not permitted information storage apparatus receives a card user's request for a change to usage permitted from a user's wireless communications terminal via the card authenticating terminal.

6. A card authentication system of any of claims 1 to 5, wherein characterized in that the usage permitted/not permitted information storage apparatus has data regarding the respective cards in advance and registers usage permitted/not permitted for the registered cards.

7. A card authentication system of any of claims 1 to 5, wherein the usage permitted/not permitted information storage apparatus registers at any time only data for those of the respective cards that are usage permitted.